XAVFSIZ KLIENT VA SERVER SOKETLARINI YARATISHDA JSSE

Jumaboyev T.A., Nizamov A.N.,Djo'rayev A.A., G'ayratov Z.K

Muhammad al-Xorazmiy nomidati TATU Samarqand filiali o'qituvchilari

Nurullayeva F.O., Nizamov O.S., Axmadjonova M.A

Muhammad al-Xorazmiy nomidati TATU Samarqand filiali talabasi

JSSE - Java Secure Socket Extensions so'zlarining qisqartmasi hisoblanadi, ya'ni Javaning Xavfsiz Soket Kengaytmasi degan ma'noni anglatadi. Nomidan kelib chiqib SSL/TLS funktsionalligini ta'minlovchi Java API lar to'plamidan iborat. JSSE klient soketlari uchun SSLSocket va server soketlari uchun SSLServerSocketlarni yaratishni ta'minlaydi.

SSL klient soket yaratish algoritmi:

1. Eshitib turgan SSL server nomi va portini aniqlash
2. JSSE provayderni ro'yxatdan o'tkazish
3. SSLSocketFactory ekzemplyarini yaratish
4. SSLSocket ekzemplyarini yaratish
5. SSL serverga yozish uchun OutputStream obyektini yaratish
6. SSL serverdan xabarlarni qabul qilish uchun InputStream obyektini yaratish

SSL server soketini yaratish algoritmi:

1. JSSE provayderni ro'yxatdan o'tkazish
2. Server sertifikatini o'z ichiga oluvchi keystore uchun tizim xususiyatlarini o'rnatish
3. Server sertifikatini o'z ichiga oluvchi keystorening paroli uchun tizim xususiyatlarini o'rnatish
4. SSLServerSocketFactory ekzemplyarini yaratish
5. SSLServerSocket ekzemplyarini yaratish
6. SSLSocket obyektini initsializatsiya qilish

7. Klientlardan jo‘natilgan ma’lumotni o‘qish uchun InputStream obyektini yaratish

8. Klientlarga ma’lumot yuborish ushun OutputStream obyektini yaratish.

Keytool zaruriyati.

Keytoolning tez-tez foydalaniladigan ba’zi funktsiyalari:

Generatsiyalangan kalitlar keytooldan foydalanishadi.

Kalitlar juftligi quyidagi buyruqlar bilan keytooldan foydalanib generatsiya qilinadi:

```
$bash # keytool -genkey -alias testkey -keystore testkeystore.ks
Enter keystore password:  Umarxodjayeva
What is your first and last name?
  [Unknown]:Nazira
What is the name of your organizational unit?
  [Unknown]: II
What is the name of your organization?
  [Unknown]:  TUIT
What is the name of your City or Locality?
  [Unknown]:  Tashkent
What is the name of your State or Province?
  [Unknown]:  Uzbekistan
What is the two-letter country code for this unit?
  [Unknown]:  UZ
Is CN=Nazira, OU=II, O=TUIT, L=Tashkent, ST=Uzbekistan, C=UZ correct?
  [no]:  y

Enter key password for <testkey>
        (RETURN if same as keystore password):
```

-genkey optsiyasi kalitlarni generatsiya qilish uchun foydalaniladi.

- *alias* kalit nomini aniqlaydi. Ushbu buyruq keytoolning -list -keystore buyruqlari bilan tekshirish
- *keystore* kalit qo‘shilishi kerak bo‘lgan keystore nomini aniqlaydi. Agar keysore nomi aniqlanmagan bo‘lsa generatsiya qilingan kalitlar sukut bo‘yicha keystorega qo‘shiladi.

Quyidagilar sukut bo‘yicha qiymatlar hisoblanadi: keyalg – DSA, keysize – 1024 bit, amal qilish muddati – 90 kun.

.cer faylidan keystorega sertifikatlarni import qilish.

```
$bash # keytool -import -keystore testkeystore.ks -file ssltest.cer
Enter keystore password:  testpwd
Owner: CN=Jane P, OU=Network Admins, O=NewCo, L=Denver, ST=CO, C=US
Issuer: CN=Jane P, OU=Network Admins, O=NewCo, L=Denver, ST=CO, C=US
Serial number: 45697b96
Valid from: Sun Nov 26 06:33:42 EST 2025 until: Wed Apr 12 07:33:42 EDT 2026
Certificate fingerprints:
        MD5:  BD:AA:A5:77:AC:92:17:0E:D3:6E:E2:8F:2B:12:A5:6C
        SHA1: 2F:BF:88:E1:2F:26:B9:C3:64:5E:C5:7F:F4:BF:43:7F:37:3D:BE:C5
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

Sertifikat tarkibini ko‘rish uchun keytool -printcert -file ssltest.cer dan foydalanish.

```
$bash # keytool -printcert -file ssltest.cer
```

Owner: CN=Jane P, OU=Network Admins, O=NewCo, L=Denver, ST=CO, C=US

Issuer: CN=Jane P, OU=Network Admins, O=NewCo, L=Denver, ST=CO, C=US

Serial number: 45697b96

Valid from: Sun Nov 26 06:33:42 EST 2025 until: Wed Apr 12 07:33:42 EDT 2034

Certificate fingerprints:

MD5: BD:AA:A5:77:AC:92:17:0E:D3:6E:E2:8F:2B:12:A5:6C

SHA1: 2F:BF:88:E1:2F:26:B9:C3:64:5E:C5:7F:F4:BF:43:7F:37:3D:BE:C5

Verify from the Issuer of the certificate if the Certificate fingerprint matches.

Keystore faylidan sertifikatlarni eksport qilish quyidagicha bo‘ladi:

$bash # keytool -export -alias testkey -keystore testkeystore.ks -file testkey.cer

Enter keystore password: 1234546

Certificate stored in file <testkey.cer>

Now you can verify the contents of the exported certificate using the command.

$bash # keytool -printcert -file testkey.cer

Owner: CN=Tom, OU=security, O=ABC Inc, L=Fort Meade, ST=MA, C=US

Issuer: CN=Tom, OU=security, O=ABC Inc, L=Fort Meade, ST=MA, C=US

Serial number: 45736152

Valid from: Sun Dec 03 18:44:18 EST 2025 until: Sat Mar 03 18:44:18 EST 2026

Certificate fingerprints:

MD5: 8F:D3:EA:E7:B0:CF:9C:03:16:2F:3F:C9:6C:BC:5A:D4

SHA1: 03:2B:C6:BD:D9:82:31:08:F1:88:3C:35:AD:8D:F9:C3:90:5E:53:6F

Keytool qo‘llab-quvvatlaydigan algoritmlar. Keytool ro‘yxatdan o‘tgan kriptografic xizmatni ta’minlovchilar tomonidan tadbiq etilgan barcha algoritmlarni qo‘llab-quvvatlaydi. Sukut bo‘yicha kalit 1024 bitli DSA algoritm asosida generatsiya qilinadi.

Xavfsiz soketlar klient va server o‘rtasidagi aloqani himoyalangan kanalda tashkil qiladi. TCP/UDP protokollari orqali ikki tomonlama ma’lumot almashinuvi amalga oshadi. Klient so‘rov yuboradi, server uni qabul qilib, tegishli javob qaytaradi. Ma’lumotlar SSL/TLS orqali shifrlanadi, bu esa ma’lumotlarni uchinchi shaxslar tomonidan o‘qilishidan himoya qiladi.

Foydalanish sohalari: chat dasturlari, fayl uzatish tizimlari, onlayn xizmatlar va moliyaviy tizimlar. Ushbu tizimlar ishlashida InputStream va OutputStream orqali ma’lumotlar uzatiladi. Nosozliklarni aniqlashda tarmoq xatolari, ulanish uzilishi yoki paket yo‘qolishi kuzatiladi. To‘g‘ri sozlangan soketlar barqaror va samarali ishlaydi.

ADABIYOTLAR RUYXATI.

1. Java Network Programming, Fourth Edition by Elliotte Rusty Harold. 2014. Published by O‘Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol.

2. Computer networking: a top-down approach / James F. Kurose, Keith W. Ross.—6th ed. 2013. by Pearson Education, Inc., publishing as Addison-Wesley.

3. TCP/IP protocol suite / Behrouz A. Forouzan.—4th ed. Published by McGraw-Hill, a business unit of The McGraw-Hill Companies, Inc., 1221 Avenue of the Americas, New York, NY 10020. Copyright © 2010

4. Support Readiness Document for Java Secure Socket Extension 1.0.1. Sun Microsystems, Inc. 901 San Antonio Road. Palo Alto, CA 94303. U.S.A. 2010.

5. Implementing SSL / TLS Using Cryptography and PKI. Joshua Davies. 2011.

6. Network Security with OpenSSL. Book by John Viega, Matt Messier, and Pravir Chandra. 3.9/5 · Shop O‘Reilly - O‘Reilly Media. 2002

7. Ристич, И. (2014). Непробиваемый SSL и TLS: Понимание и внедрение SSL/TLS и PKI для защиты серверов и веб-приложений. Feisty Duck.